Internet-Sicherheit von Windows-Rechnern

Das Internet ist in den letzen Jahren explosionsartig gewachsen. Die International Data Corporation (IDC) schätzt, daß im Jahr 2000 zweihundert Millionen Menschen das Internet nutzen werden – 1995 waren es ca. 35 Millionen. Jede Minute, jeden Tag verbinden sich weltweit immer neue Rechner oder ganze Netzwerke mit dem Internet. Laut einer Zählung, die von den „Network Wizards" im Internet durchgeführt wurde, gab es im Juli '97 im DNS-Adressraum 19.540.000 Rechner. Ein Jahr zuvor waren es noch 12.881.000. Es scheint, daß sich jeder mit dem „Netz der Netze" verbinden möchte. Die einfache Unterstützung der populärsten Internet-Protokolle durch Windows NT und Windows 95 tut ihr übriges: TCP/IP Protokoll laden, Router konfigurieren, einen Internet Provider aussuchen, und bevor der Nutzer es merkt, ist er Bestandteil des Internet – und somit potentielles Angriffsziel, wie die restlichen 19 Millionen Rechner.

Der so einfach ans Internet angeschlossene Rechner ist durch eben diese Verbindung nun neuen Gefahren ausgesetzt. Zu diesem Zeitpunkt hat der Nutzer sicherlich noch keine Vorstellung davon, wie es ist, am Sonntagmorgen um drei im Rechenzentrum nach „sauberen" und aktuellen Backups suchen zu müssen, weil ein Hacker seine, bzw. ihre, Hand im internen Netzwerk hatte. Der folgende Artikel soll Ihnen zeigen, wie Sie diesen Alptraum verhindern können.

Eigentlich hat der sicherste Rechner keine Netzwerkkarte, keine Festplatte, ist ausgeschaltet und steht in einem verschlossenen, bewachten Raum. Leider ist dies nicht sehr sinnvoll. Ebensowenig sinnvoll ist allerdings ein ungesichertes System, das an das Internet angeschlossen ist und jedem anonymen Zugang zu seinen Ressourcen gestattet. Bevor Sie also Ihren Windows-Rechner an das Internet anschließen, sollten Sie wissen, wie Sie verhindern können, daß Ihre Daten gefährdet werden. Sie sollten genau planen, welchen Rechner Sie an das Internet anschließen und welche Daten sich darauf befinden sollen.
Sie sollten im Vorfeld

- herausfinden, was Sie zu schützen beabsichtigen,
- wissen, was Sie für diesen Schutz benötigen,
- bestimmen, welcher Aufwand für diesen Schutz notwendig ist,
- Maßnahmen einleiten, die Sie kostengünstig schützen und
- Ihre Entscheidungen kontinuierlich überprüfen, um Ihre Schutzmaßnahmen den wechselnden Anforderungen anzupassen.

Bevor Sie sich nach Software umsehen, die Ihre Systemsicherheit erhöhen soll, nutzen Sie zuerst die Mittel und Methoden, die Ihnen Ihr Betriebssystem selbst liefert.

Windows NT bietet Schutzmöglichkeiten in vier grundlegenden Bereichen:

- log-on Authentisierung,
- Objektsicherheit,
- Nutzerrechte,
- Audit.

Wenn Sie diese Bereiche gut konfiguriert haben, sind Sie bestens für einen Anschluß an ein öffentliches Netzwerk gewappnet. Hier sind ein paar Tips, wie Sie Ihr NT/95-Netzwerk zu einem sicheren Bereich machen können.

Diese Liste ist wie immer unvollständig und soll als kleine Gedächtnisstütze dienen. Sie zeigt nur einen Teil der Dinge auf, über die Sie nachdenken sollten, wenn Sie Ihren Windows-PC oder Ihr Windows-Netzwerk an das Internet anschließen wollen.

1. Sie sollten `NTFS`- dem `FAT`-Dateisystem vorziehen. `NTFS` hat Sicherheitseigenschaften, die `FAT` nicht besitzt. Müssen Sie `FAT` aus irgendeinem Grund doch einsetzen, sollten keine Systemdateien auf diesem Dateisystem vorhanden sein. Sensitive Daten sollten ebenfalls nicht auf einem `FAT`-Dateisystem gespeichert werden. Sie können keine Zugriffs- und Eigentümerrechte an Dateien auf `FAT`-Dateisystemen definieren. Beim Exportieren solcher Dateisysteme ist der ganze Verzeichnisbaum gefährdet.
2. Stellen Sie sicher, daß alle betriebssystemeigenen Paßwortschutzoptionen aktiviert sind. Dies beinhaltet zwingend ein schwer zu erratendes Paßwort und sein Wechseln in regelmäßigen Zeitabständen. Auch ist es ratsam, den Namen des letzen angemeldeten Nutzers beim nächsten Logon zu verbergen. Windows NT kann Nutzerkonten automatisch sperren, nachdem mehrere falsche Paßwörter eingegeben wurden. Aktivieren Sie diese Option. Sie können damit verhindern, daß sich ein Eindringling durch sogenannte Brute Force Attacks Zugang zu Ihrem System veschafft. Fordern Sie Ihre Nutzer auf, schwer zu erratende Paßwörter zu wählen *(siehe RZM 12 -Accounts und Paßwörter*). Solange Microsoft nicht die Verschlüsselung der `SAM`-Datenbank (Security Account Manager) ändert, ist es ratsam, Paßwörter von zwischen sechs bis acht Zeichen Länge zu wählen. Dies erhöht die Zeit, die ein Eindringling braucht, um ein Paßwort zu erraten. Brute Force Attacks auf Paßwörter sind heute eine sehr populäre Methode, um in Netzwerke einzudringen. Es ist ebenfalls ratsam, die Datei `PASSFILT.DLL` zu installieren, die mit dem Windows NT Servicepack 2 und 3 ausgeliefert wird. Sie können mehr über diese DLL in den Microsofts Knowledge Base-Artikeln und den `README`-Dateien der Servicepacks erfahren.

3. Es ist kein Geheimnis, daß der Administrator-Account Ziel für die meisten Angriffe ist. Erstellen Sie einen neuen Administrator-Account und übertragen Sie alle Rechte vom existenten Administrator-Account auf den neuen. Geben Sie diesem neuen Account einen unscheinbaren Namen. Entziehen Sie dem alten Administrator-Account alle Rechte, löschen Sie ihn jedoch nicht. Ein Eindringling wird sehr viel Zeit aufwenden, in diesen Account einzubrechen.
4. Verringern Sie die Zahl der Nutzer, die zur Administratorgruppe gehören. Erteilen Sie niemandem aus Bequemlichkeit Administratorrechte und überprüfen Sie die Mitglieder der Administratorgruppe regelmäßig.
5. Aktivieren Sie das Auditsystem auf allen Windows NT Rechnern. Im Bereich Audit im User Manager können Sie eine Audit Policy für jeden Nutzer oder jede Nutzergruppe definieren. Mit Hilfe des Explorers können Sie ein objektbezogenes Audit konfigurieren.
6. Seien Sie sehr vorsichtig beim Aktivieren von `NT Domain Trusts`. Diese Konfigurationen können in größeren NT-Netzwerken schnell außer Kontrolle geraten, zumal, wenn dieses Vertrauen wechselseitig besteht.
7. Deaktiveren Sie `NetBIOS über TCP/IP`, wo immer Sie können. Dies betrifft besonders Ihre Windows-Rechner, die als Gateway zum Internet dienen.
8. Deaktivieren Sie alle nicht benötigten TCP/IP Ports (`Inbound` und `Outbound`). Achten Sie besonders darauf, daß die UDP Ports `137` und `138` und der TCP Port `139` auf Ihren Gateways, Routern und Firewall-Systemen blockiert werden. Dies verhindert bekannte und auch neue Attacken aus dem Internet auf Ihr Windows-Netzwerk.
9. Deaktivieren Sie die Option `Access from Network` (mittels des `User Managers`) für alle Nutzer, die diesen Zugang nicht unbedingt benötigen. Diese Nutzer können dann nur noch lokal an der Konsole arbeiten.
10. Überprüfen Sie in regelmäßigen Zeitabständen Ihr System auf überflüssige Nutzer-Accounts. Setzen Sie für alle temporären Accounts ein Verfallsdatum und erteilen Sie Rechte vorsichtig.
11. Informieren Sie Ihre Nutzer durch Hinweise beim Logon, daß der Zugang zu Ihren Systemen nur authorisierten Nutzern gestattet ist, daß Protokollierungen stattfinden und jeder Verstoß gegen Ihre Sicherheitsrichtlinien überprüft und gegebenenfalls juristisch verfolgt wird. In vielen Fällen ist es selbst in Ihrem privaten Netzwerk datenschutzrechtlich bedenklich, Netzverbindungsdaten zu protokollieren und auszuwerten. Dieser Hinweis könnte Sie vor juristischen Problemen schützen. Die Warnung sollte nicht nur auf Ihrem Logon-Bildschirm, sondern auch auf Ihren WWW- und FTP-Servern erscheinen.
12. Stellen Sie sicher, daß Ihre Nutzer ihre Windows-Workstations nicht im eingeschalteten Zustand unbeaufsichtigt lassen. Überall sollten paßwortgeschützte Bildschirmschoner aktiviert sein. Erziehen Sie Ihre Nutzer dazu, sich abzumelden, wenn Sie für längere Zeit die Workstation verlassen. Es ist auch ratsam, die Windows-Workstations über Nacht und an Wochenenden auszuschalten. Dies könnte helfen, die Zahl der illegalen Modem-, FTP- und WWW-Server einzudämmen.
13. Ein Gast-Account wird bei jeder Windows NT-Installation automatisch eingerichtet. Wenn möglich, sollten Sie diesen Account entfernen. Bei Bedarf sollten Sie sich die Zeit nehmen, einen temporären Gast-Account zu erstellen. Wenn Sie den Microsoft Internet Information Server (IIS) installieren, wird automatisch ein spezieller Gast-Account `IUSR_Rechnername` eingerichtet. Dieser Nutzer kann sich lokal anmelden. Wenn Sie keinen anonymen Zugriff auf Ihren WWW-Server haben wollen, sollten Sie diesen Account entfernen.
14. Überwachen Sie Ihr Netzwerk engmaschig. Es gibt immer wieder Fälle, bei denen ein Einbruch nicht bemerkt wird, weil kein Netzmonitor oder Intruder Detection System im Netzwerk installiert war.
15. Stellen Sie sicher, daß die Router und Gateways zwischen Ihrem privaten und dem öffentlichen Netzwerk `Source Routing`, `IP Spoofing` und `ICMP Redirects` verhindern können und es auch tun. Es kann auch nicht schaden, Software einzusetzen, die einen Netzwerkscan aus dem Internet verhindert.
16. Deaktivieren Sie die einfachen TCP/IP-Dienste auf Ihrem Windows Rechner. Dies stoppt Dienste wie `chargen`, `echo`, `daytime`, `discard` und `qotd`. Diese Dienste eignen sich exellent, um Ihren Rechner mit einer Denial-of-Service Attack lahmzulegen.
17. Auf Ihrem Windows-Rechner sollten keine Dienste laufen, die Sie nicht unbedingt brauchen. Solche Dienste sind immer wieder gezielten Attacken ausgesetzt.
18. Versuchen Sie, Ihre Nutzer zum Mitdenken zu erziehen. Führen Sie regelmäßig Schulungen und Weiterbildungen durch.

Ausgehend vom derzeitigen Entwicklungstand, sollten Sie diese Hinweise beachten, bevor Sie einen Windows 95- oder Windows NT-Rechner ungeschützt mit einem öffentlichen Netz wie dem Internet verbinden.

Alexander Geschonneck
geschonneck@rz.hu-berlin.de
www.hu-berlin.de/~h0271cbj/